IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS 25 VARNEY STREET, APARTMENT 2, MANCHESTER, NEW HAMPSHIRE; THE PERSON OF NORMAN BOLDUC AND ANY OTHER PERSON(S) PRESENT AT THE SUBJECT PREMISES; AND A BLUE 2008 SUBARU OUTBACK BEARING NEW HAMPSHIRE REGISTRATION 421 9649	Case No. 1:22-mj- 215-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search (A) the premises and property located at 25 Varney Street, Apartment 2, Manchester, New Hampshire (the "SUBJECT PREMISES"), further described in Attachment A; (B) the person of Norman Bolduc and any other person(s) present at the SUBJECT PREMISES; (C) a blue 2008 Subaru Outback bearing New Hampshire registration 421 9649 (the "SUBJECT VEHICLE"); and (D) any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during the course of said searches. Located within the places and items to be searched, I seek authorization to seize evidence, fruits, and instrumentalities relating to violations of 18 U.S.C. §§ 2252A(a)(2)

[distribution and/or receipt of child pornography] and 2252A(a)(5) [possession of child pornography] (the "SUBJECT OFFENSES"), as more fully described in Attachment B.

2. I am a detective with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I have also completed HSI's Task Force Officer Course. I hold a bachelor's degree in criminal justice, with a minor in computer science and victimology, from Endicott College.

3. Since November 2019, I have been assigned to the Special Investigations Division as a member of the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a TFO, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a TFO and a member of the ICAC, I investigate criminal violations related to online sexual exploitation of children.

4. I have received training in the areas of online child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations and using undercover personas on various social media applications for proactive investigations. I have also attended the National Law

Enforcement Conference on Child Exploitation where I took classes on using undercover personas, IRC investigations, and investigations on BitTorrent and the Freenet. I have personally conducted numerous online undercover investigations using social media applications such as KIK messenger, Grindr, WhatsApp, Whisper, and MeetMe along with investigation on peer-to-peer ("P2P") networks. Furthermore, I have completed additional trainings offered by the Internet Crimes Against Children Task Force, National Training Program which is a program of the Fox Valley Technical College – National Criminal Justice Training Center, on BitTorrent investigations, to include the BitTorrent Overview, ICAC BitTorrent Update and Refresher, Corroborating BitTorrent Investigations, and interview techniques in P2P investigations. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics.

5. In the course of investigating crimes related to the online sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous online child sexual exploitation investigations and am very familiar with the tactics used by offenders who collect child sexual exploitation materials and those who seek to exploit children.

6. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience. In addition, over the course of this investigation, I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses.

7. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of the SUBJECT OFFENSES have been committed, are being committed, and will be committed by individual(s) residing within the SUBJECT PREMISES. There is also probable cause to believe that evidence, contraband, fruits, and instrumentalities of the SUBJECT OFFENSES are at the SUBJECT PREMISES, on the person of Bolduc and/or other individual(s) within the SUBJECT PREMISES, and/or in the SUBJECT VEHICLE.

BACKGROUND ON PEER-TO-PEER (P2P) SOFTWARE

9. Peer-to-peer ("P2P") file-sharing is a method of communication available to Internet users through the use of special software such as BitTorrent. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

10. BitTorrent is one type of P2P file-sharing protocol. Users of the BitTorrent network wishing to share new content will use a BitTorrent client to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash," which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

11. For example, a person interested in obtaining child pornographic images would open a torrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a .torrent from the results displayed the file(s) he/she wants to download. Once the .torrent file is downloaded, it is used by a BitTorrent program which the user had previously installed. The .torrent file is the set of instructions the program needs to find the files referenced in the .torrent file. The file(s) is downloaded directly from the computer or computers sharing the file. The downloaded file(s) is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

12. One of the advantages of P2P file-sharing is that multiple files may be downloaded at the same time. This means that the user can download more than one file at a time. In addition,

a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

13. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

14. The computer running the file sharing application, in this case a Bittorrent application, has an IP address assigned to it while it is on the internet. Through the law enforcement software, investigators can see the IP address of any computer system sharing files with them. The law enforcement software logs the IP address which has sent them files or information regarding files being shared. Investigators can then search public records that are available on the internet to determine the internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the internet service provider.

15. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once someone checks a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

PROBABLE CAUSE

16. The Nashua Police Department ("NPD") maintains a law enforcement version of the BitTorrent software for use in undercover investigations into online child sexual exploitation. The UC BitTorrent software uses SHA1 hash values to identify files being shared on the network that have been previously determined to contain child pornography and/or related material. When the software recognizes the SHA1 hash value of such files on the network, it automatically tries to download them. Further, the BitTorrent software used by law enforcement uses a single-source download protocol. In other words, when the software identifies a BitTorrent user that has suspected files of child pornography available for download, it will initiate a download of the entire file from that single user, as opposed to downloading portions of the target file from multiple users. This tool allows investigators to focus on users sharing child sexual abuse material on the BitTorrent Network.

17. In June 2022, while monitoring NPD's BitTorrent software, Detective Peter LaRoche and I began observing downloads of suspected child pornography materials from IP address [redacted].34, which resolved to Manchester, New Hampshire.

18. For example, on June 3, 2022, at approximately 21:54:45 UTC, the UC BitTorrent software identified a torrent [redacted]4180, with a SHA1 info hash that had been previously determined to contain child sexual exploitation materials, that was available for download from IP address [redacted].34. The UC BitTorrent software connected with the target IP address and the target IP address acknowledged it had pieces 817-872, which encompassed all of file 11, file 24, file 25, file 28, and file 31. I reviewed the filenames of the previously mentioned files and based on the names, believed they contained child exploitation materials. The UC BitTorrent software completed a single-source download from the user

connected to the target IP address and downloaded four pieces of file 31, which was filename "Voyeur school girl toilet piss hidden cam private PTHC girl child pedo 4yo 5yo 6yo 7yo 8yo 9yo 10yo.mpeg," a four-minute and fifteen-second video of a hidden camera zooming in on various female children's vaginal area as they urinated into a toilet. Although only four "pieces" were downloaded, I note the file played fully on the UC BitTorrent computer.

19. I later observed the NPD BitTorrent software had a copy of the torrent [redacted]4180. I reviewed the copy and observed it contained child sexual exploitation material. For example, among the files from this torrent download was filename "(PTHC) Kelly 8Yo - Sucking & Trying Fuck.avi," a three-minute and four-second video depicting a nude prepubescent female and adult male engaging in oral sex before transitioning into the male rubbing/inserting his penis on/in the prepubescent female's anal/vaginal openings.

20. Using additional investigative techniques, I learned that FBI Special Agent Virginia Bend had also connected to the IP address [redacted]34 on June 3, 2022, at 20:59:40 UTC, via an undercover BitTorrent account. SA Bend's UC BitTorrent software identified a torrent of investigative interest, [redacted]b3fe9, that was available for download from the IP address [redacted]34. The SHA1 info hash associated with the torrent was one that had been previously determined to contain child sexual exploitation material. The UC BitTorrent software connected with the target IP address and successfully downloaded one file. The file is described as:

Filename: ProjectNew – PTHC – hard anal play (low q).mp4

Description: three-minute and twenty-five second video involving a naked prepubescent female and naked adult male. The prepubescent female starts off lying on her back with her legs open, exposing her vaginal area. The male proceeds to position himself in

between the female's legs and appears to be inserting his penis into the prepubescent female's vaginal or anal opening.

21. Pursuant to a summons for IP address 7[redacted]34, Comcast Cable Communications identified the subscriber as [redacted] of 25 Varney Street, Apartment 2, Manchester, New Hampshire.

22. Since June 3, 2022, I have not observed any additional BitTorrent activity resolving to IP address[redacted].34.

23. Using various databases, I identified [redacted], Norman Bolduc, and [redacted] as possible residents of the SUBJECT PREMISES.

24. On August 3, 2022, Manchester Police Department Officer David Labbe, who works in the sex offender compliance unit, confirmed that two registered sex offenders, [redacted] and Norman Bolduc, reported their then-current address as 25 Varney Street, Apartment 2, Manchester, New Hampshire (the SUBJECT PREMISES).

25. Officer Labbe provided me with [redacted] and Bolduc's most recent sex offender registrations (SOR) completed on June 3, 2022 (Bolduc) and July 6, 2022 ([redacted]). Upon reviewing the SORs, I observed both listed their legal address as 25 Varney Street, Apartment 2, Manchester, NH. Bolduc is a registered sexual offender in New Hampshire due to a 2010 conviction for possession of child pornography. [redacted] is a registered sexual offender in New Hampshire due to a 2011 conviction of aggravated felonious sexual assault.

26. Officer Labbe provided me with a report completed by the Manchester Police Department in June 2022, which involved [redacted] not properly reporting his residence. According to the Manchester Police report, [redacted] claimed to reside at 25 Varney Street, Apartment 2, Manchester, New Hampshire. Officer Ryan White conducted a compliance

check at the SUBJECT PREMISES on June 15, 2022, and he learned that Bolduc and his girlfriend, [redacted], reside at the residence. Bolduc advised that [redacted] only stayed at the apartment one or two nights a week and primarily resided in Concord, New Hampshire. As a result of that investigation, [redacted] was arrested on July 8, 2022, and he has been incarcerated at the New Hampshire State Prison since that date.

27. During the months of August, September, and October 2022, while conducting intermittent surveillance of the SUBJECT PREMISES, I have observed the SUBJECT VEHICLE, which is registered to Bolduc, parked in small private parking lot for residents behind the building. I have further observed Bolduc leave the SUBJECT PREMISES and drive away in the SUBJECT VEHICLE around 6:30 a.m. on weekdays. According to Bolduc's sex offender registration form, Bolduc is employed by a business in Manchester. Based on the time Bolduc leaves and the route he takes, it appears he is leaving his residence and traveling to work when I have observed him leaving around 6:30 a.m. During surveillance, I have not observed any vehicles registered to [redacted] or [redacted]

28. In addition, while conducting intermittent surveillance at the SUBJECT PREMISES, I scanned for wireless signals in the area and observed 32 Wi-Fi networks with 31 of those secured (i.e., require a password to access). I noted that the unsecured Wi-Fi network was a Wi-Fi hotspot serviced by Comcast.

29. I have reviewed reports from Manchester Police Department related to Bolduc's prior conviction for possession of child pornography. According to the report, in 2009, Bolduc's then-girlfriend located child sexual exploitation images on a computer that she loaned to Bolduc. In the course of that investigation, Bolduc admitted using FrostWire, another P2P application, to download child pornography. Bolduc estimated he had downloaded five to ten files of child sexual

exploitation, but he was unsure on the exact number. A forensic review of the computer showed approximately twelve files of child sexual exploitation.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found at the SUBJECT PREMISES, on the person of Norman Bolduc and/or on any person(s) located within the SUBJECT PREMISES, and/or in the SUBJECT VEHICLE. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during the course of said searches, and potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer or other electronic storage medium is found on the SUBJECT PREMISES, on the person of Norman Bolduc and/or on any person(s) located within the SUBJECT PREMISES, and/or in the SUBJECT VEHICLE, there is probable cause to believe those records will be stored on that computer or electronic storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as

Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

CHARACTERISTICS OF CHILD PORNOGRAPHY OFFENDERS

71. As set forth above, probable cause exists to believe that an individual at the SUBJECT PREMISES has distributed, received, and/or possessed child pornography. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, in the privacy and security of their home or some other secure location.

c. Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

72. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer on the SUBJECT PREMISES, on the person of Norman Bolduc and/or on any person(s) located within the SUBJECT PREMISES, and/or in the SUBJECT VEHICLE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as

a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed

along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

73. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

74. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The nature of evidence**. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. **The volume of evidence**. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. **Technical requirements**. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know

before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. **Variety of forms of electronic media**. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

75. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

76. This warrant seeks authorization for law enforcement to compel Norman Bolduc and/or any person(s) located within the apartment to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

77. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition

features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

78. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

79. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

80. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the

registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

81. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

82. As discussed in this affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

83. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked fora certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric

features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

84. In light of the foregoing, and with respect to (1) any device found on the person of Norman Bolduc, (2) any device found on other individuals within the apartment (3) any device at/in the SUBJECT PREMISES reasonably believed to be owned, used, or accessed by Norman Bolduc or any person(s) located within the apartment or (4) any device in the SUBJECT VEHICLE reasonably believed to be owned, used, or accessed by Norman Bolduc, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of Norman Bolduc or any person(s) located within the apartment to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of Norman Bolduc or any person(s) located within the apartment and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of Norman Bolduc or any person(s) located within the apartment and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

85. The proposed warrant does not authorize law enforcement to compel that Norman Bolduc or any person(s) located within the apartment or any other individual present at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel Norman Bolduc or any person(s) located within the apartment or any other individual present at the SUBJECT PREMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

86. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crimes of distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B), may be located within the SUBJECT PREMISES, on the person of Norman Bolduc or on the person of any person(s) located within the apartment, and/or within the SUBJECT VEHICLE. I therefore seek a warrant to search the SUBJECT PREMISES, the person of Norman Bolduc or any person(s) located within the apartment, and the SUBJECT VEHICLE, and to seize and search the items described in Attachment B.

87. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later identified by a computer forensic examiner.

Attested to by the Affiant:

/s/ Adam Rayho
Adam Rayho, Task Force Officer
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Oct 12, 2022
Time: 12:23 PM, Oct 12, 2022

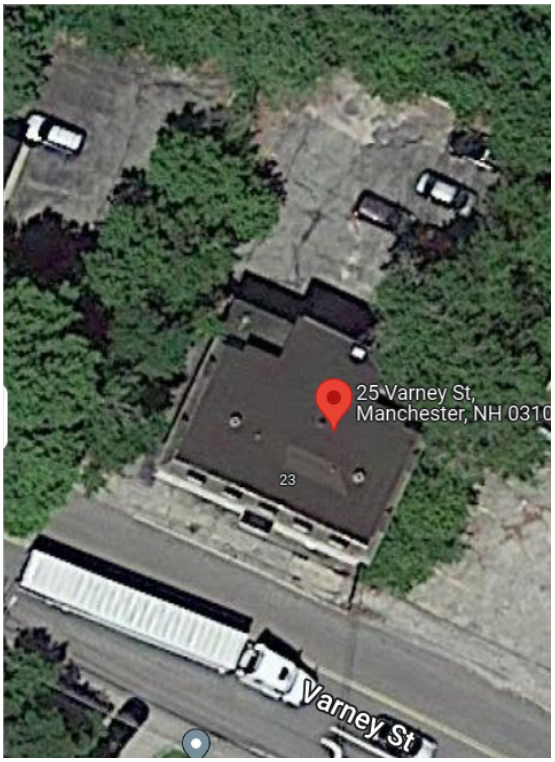
/s/ Andrea K. Johnstone
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PLACES, PERSONS, AND ITEMS TO BE SEARCHED

The places, persons, and items to be searched are (A) the premises and property located at 25 Varney Street, Apartment 2, Manchester, New Hampshire (the "SUBJECT PREMISES"), to include all rooms, attics, closed containers, and other places therein, including garages, storage areas, utility sheds, mailboxes, and trash containers under the control of the occupants of the SUBJECT PREMISES; (B) the person of Norman Bolduc and any other person(s) present at the SUBJECT PREMISES; (C) a blue 2008 Subaru Outback bearing New Hampshire registration 421 9649 (the "SUBJECT VEHICLE"); and (D) any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during the course of said searches.

The SUBJECT PREMISES is depicted below and described as a multi-family apartment building which is tan in color and displays "25" to the left of the front door. Apartment 2 is located on the first floor. A door on the back side of the residence displays the number "2," which has been used by law enforcement to access the apartment to speak with Bolduc in the past. The following photograph depicts the front of the SUBJECT PREMISES and the overhead view of the SUBJECT PREMISES.



ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized includes all information and objects that constitute fruits, contraband, evidence and instrumentalities of violations 18 U.S.C. §§ 2252A(a)(2) [receipt and/or distribution of child pornography] and 2252A(a)(5)(B) [possession of child pornography], in any form wherever they may be stored or found at the SUBJECT PREMISES, on the person of Norman Bolduc or any other persons present, and the SUBJECT VEHICLE including:

1. Computers[1] or storage medium[2] used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. Evidence of the lack of such malicious software;
    d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
    e. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
    f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
    g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
    h. Evidence of the times the COMPUTER was used;
    i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

---

[1] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

[2] The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, compact discs, memory cards, memory chips, and other magnetic or optical media.

j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. Records of or information about Internet Protocol addresses used by the COMPUTER;
l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
m. Contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, child erotica, and other images of children, including photographs, drawings, sketches, fantasy writings, and notes showing an interest in unlawful sexual contact with children, and evidence assistance authorities in identifying any such children;

5. Internet history, including evidence of visits to websites and applications that offer visual depictions of minors engaged in sexually explicit conduct or that offer a platform to communicate with others who are interested in unlawful sexual contact with children, including evidence of peer-to-peer (P2P) file sharing programs including BitTorrent;

6. Correspondence and records regarding engaging in, or enticing others to engage in sexually explicit conduct with minors, including envelopes, letters, mailings, electronic mail, chat logs, electronic messages on messaging applications, books, ledgers, and records of communications with other individuals, including on any child exploitation bulletin boards, chat forums, or organizations;

7. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence; and

8. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

Biometric Access: During the execution of the search of the SUBJECT PREMISES, the person of Norman Bolduc and any other person(s) present at the SUBJECT PREMISES, and the SUBJECT VEHICLE, all described further in Attachment A, law enforcement personnel are

authorized to: (1) press or swipe the fingers (including thumbs) of Bolduc, and any other occupants found at the SUBJECT PREMISES to the fingerprint scanner of the devices; (2) hold the devices in front of the face of Norman Bolduc, and any other occupants found at the SUBJECT PREMISES, and activate the facial recognition feature; and/or (3) hold the devices in front of the face of Norman Bolduc, and any other occupants found at the SUBJECT PREMISES, and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.